

ABSTRACT OF THE DISCLOSURE

The principles of the present invention relate to systems, methods, and computer program products for more efficiently and securely authenticating computing systems. In some embodiments, a limited use credential is used to provision more permanent credentials. A client receives a limited-use (e.g., a single-use) credential and submits the limited-use credential over a secure link to a server. The server provisions an additional credential (for subsequent authentication) and sends the additional credential to the client over the secure link. In other embodiments, computing systems automatically negotiate authentication methods using an extensible protocol. A mutually deployed authentication method is selected and secure authentication is facilitated with a tunnel key that is used encrypt (and subsequently decrypt) authentication content transferred between a client and a server. The tunnel key is derived from a shared secret (e.g., a session key) and nonces.

W:\13768\497\MBD0000000278V001.doc

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111